AMENDMENTS TO THE CLAIMS

1. (Currently amended) A quantum cryptographic system comprising:

~~at least one~~ a sending unit comprising an encoder and configured to distribute a raw key in the quadrature components of quantum coherent states ~~that are continuously modulated~~ by modulating the quantum coherent states with a continuous distribution in phase and amplitude;

~~at least one~~ a receiving unit comprising a homodyne detector of the quantum coherent states ~~in order~~ configured to measure the quadrature components of the states and to receive the raw key;

a quantum channel for connecting the sending unit to the receiving unit; and

a two-way authenticated public channel for transmitting non-secret messages between the sending unit and the receiving unit.

2. (Original) The quantum cryptographic system of Claim 1, further comprising a continuous-variable quantum key distribution protocol ensuring that the amount of information a potential eavesdropper may gain at most on the sent and received data can be estimated from the measured parameters of the quantum channel (error rate and line attenuation).

3. (Currently amended) The quantum cryptographic system of Claim 2, wherein the ~~sent and received~~ raw ~~data~~ key resulting from the continuous-variable protocol ~~are~~ is converted into a secret binary key by using a continuous reconciliation protocol supplemented with privacy amplification.

4. (Currently amended) The quantum cryptographic system of Claim 1, wherein the encoder of the quadrature components ~~with a high signal-to-noise ratio encodes~~ is configured to encode ~~several~~ a plurality of key bits per coherent light pulse.

5. (Canceled).

6. (Currently amended) The quantum cryptographic system of Claim 3, wherein the continuous reconciliation protocol is a direct reconciliation protocol, which allows the receiver to

discretize and correct its data according to the sent values~~, in case of noisy quantum channels with low losses~~.

7. (Currently amended) The quantum cryptographic system of Claim 3, wherein the continuous reconciliation protocol is a reverse reconciliation protocol, which allows the sending unit to discretize and correct its data according to the values measured by the receiver~~, in case of noisy quantum channels with high losses~~.

8. (Original) The quantum cryptographic system of Claim 3, wherein the secret key is used as a private key for ensuring confidentiality and authentication of a cryptographic transmission.

9. (Original) The quantum cryptographic system of Claim 1, wherein the quadrature components of the quantum coherent states are modulated with a Gaussian distribution.

10. (Original) The quantum cryptographic system of Claim 9, wherein the co-ordinate values of the center of the Gaussian distribution are arbitrary.

11. (Original) The quantum cryptographic system of Claim 9, wherein the variance of the Gaussian distribution for the quadrature X is different from the variance of the Gaussian distribution for the conjugate quadrature P.

12. (Currently amended) The quantum cryptographic system of Claim 9, wherein the Gaussian-modulated coherent states are attenuated laser light pulses ~~typically containing several photons~~.

13. (Original) The quantum cryptographic system of Claim 12, wherein the information an eavesdropper may gain on the sent and received Gaussian-distributed values are calculated explicitly using Shannon's theory for Gaussian channels.

14. (Currently amended) A method of distributing continuous quantum key between two parties which are a sender and a receiver, the method comprising:

selecting, at a sender, two random numbers x_A and p_A from a Gaussian distribution of mean zero and variance $V_A N_0$, where N_0 refers to the shot-noise variance;

sending a corresponding coherent state $|x_A+ip_A>$ in the quantum channel;

randomly choosing, at a receiver, to measure either quadrature x or p using homodyne detection;

informing the sender about the quadrature that was measured so the sender may discard the ~~wrong one~~ quadrature x or p that was not measured;

measuring channel parameters on a random subset of the sender's and receiver's data, in order to evaluate the maximum information acquired by an eavesdropper; and

converting the resulting raw key, which is in the form of a set of correlated Gaussian variables, into a binary secret key, the converting comprising:

direct or reverse reconciliation in order to correct ~~the~~ errors and to get a binary key, and

privacy amplification in order to make secret the binary key.

15. (Currently amended) The method of Claim 14, wherein the reconciliation produces a common bit string from correlated continuous data, ~~which comprises the following~~ the reconciliation comprising:

transforming each Gaussian key element of a block of size n by the sender into a string of m bits, giving m bit strings of length n, referred to as slices;

converting, by the receiver, the measured key elements into binary strings by using a set of slice estimators; and

sequentially ~~reconciliating~~ reconciling the slices by using an implementation of a binary error correction algorithm, and communicating on the public authenticated channel.

16. (Currently amended) The method of Claim 14, wherein the post-processing of privacy amplification comprises distilling a secret key out of the ~~reconciliated~~ reconciled key by use of a random transformation taken in a universal class of hash functions.

17. (Currently amended) A device for implementing a continuous-variable quantum key exchange, the device comprising:

a light source or a source of electromagnetic signals configured to generate short quantum coherent pulses ~~at a high repetition rate~~;

an optical component configured to ~~continuously~~ modulate with a continuous distribution the amplitude and phase of the pulses ~~at a high frequency~~;

a quantum channel configured to transmit the pulses from an emitter to a receiver;

a system that permits the transmission of a local oscillator pulse from the emitter to the receiver;

a homodyne detector capable of measuring~~, at a high acquisition frequency,~~ any quadrature component of the electromagnetic field collected at the receiver's station;

a two-way authenticated public channel that is used to ~~communicating~~ communicate non-secret messages in postprocessing protocols; and

a computer at the emitter's and receiver's stations that drives or reads the optical components and runs the postprocessing protocols.

18. (Currently amended) The device of Claim 17, wherein a local oscillator pulse is transmitted together with the signal pulse into one pulse by use of a polarization encoding system whereby each of the one pulse comprises a ~~strong~~ relatively stronger local oscillator pulse and a ~~weak~~ relatively weaker orthogonally-polarized signal pulse with modulated amplitude and phase.

19. (Original) The device of Claim 18, wherein if polarization encoding is used, the receiving system relies on polarization-mode homodyne detection requiring a quarter-wave plate and a polarizing beam splitter.

20. (Currently amended) A device for exchanging Gaussian key elements between two parties, which are a sender and a receiver, the device comprising:

a laser diode associated with a grating-extended external cavity, the laser diode configured to send light pulses ~~at a high repetition rate~~, each pulse ~~typically~~ containing ~~several~~ a plurality of photons, each pulse being ~~and is continuously~~ modulated with a continuous distribution in phase and amplitude;

an integrated electro-optic amplitude modulator and a piezoelectric phase modulator, configured to generate randomly-modulated light pulses, the data being organized in bursts of pulses;

a beam-splitter to separate the quantum signal from a local oscillator pulse; and

a homodyne detector combining the quantum signal and local oscillator pulses in order to measure one of the two quadrature components of the light field.

21. (Currently amended) The device of Claim 20, further comprising an acquisition board and a computer on the sender's and receiver's sides in order to run ~~the~~ post-processing protocols.

22. (Currently amended) The device of Claim 20, wherein the laser operates at a wavelength ~~comprised~~ between about 700 and about 1600 nm.

23. (Original) The device of Claim 20, wherein the laser operates at a wavelength comprising telecom wavelengths between about 1540 and about 1580 nm.

24. (Original) The method of Claim 14, wherein informing the sender comprises utilizing a public authenticated channel by the receiver to inform the sender.

25. (Original) The method of Claim 14, wherein the channel parameters include an error rate and a line attenuation.

26. (Currently amended) The device of Claim 17, ~~additional~~ additionally comprising:

means for selecting, at the emitter, two random numbers x_A and p_A from a Gaussian distribution of mean zero and variance $V_A N_0$, where N_0 refers to the shot-noise variance;

means for sending a corresponding coherent state $|x_A+ip_A>$ in the quantum channel;

means for randomly choosing, at the receiver, to measure either quadrature x or p using homodyne detection;

means for informing the emitter about the quadrature that was measured so the emitter may discard the ~~wrong one~~ quadrature x or p that was not measured;

means for measuring channel parameters on a random subset of the emitter's and receiver's data, in order to evaluate the maximum information acquired by an eavesdropper; and

means for converting the resulting raw key, in the form of a set of correlated Gaussian variables, into a binary secret key, the converting comprising direct or reverse reconciliation in order to correct ~~the~~ errors and to get a binary key, and privacy amplification in order to make secret the binary key.

27. (Previously presented) The method of Claim 14, wherein the sending comprises sending the corresponding coherent state $|x_A+ip_A>$ that is continuously modulated in phase and amplitude in the quantum channel.

28. (Currently amended) The ~~method~~ device of Claim 17, wherein the light source or the source of electromagnetic signals comprises the light source or the source of electromagnetic signals configured to generate~~, at a high repetition rate,~~ short quantum coherent pulses that contain ~~many~~ a plurality of photons and that are ~~continuously~~ modulated with a continuous distribution in phase and amplitude.

29. (Currently amended) The method of Claim 20, wherein each light pulse sent by the laser diode contains ~~several~~ a plurality of photons and is continuously modulated in phase and amplitude.

30. (Canceled)

31. (Canceled)

32. (Canceled)